

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-51439

(43) 公開日 平成10年(1998) 2月20日

(51) IntCl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/10			H 0 4 L 9/00	6 2 1 A
G 0 9 C 1/00	6 6 0	7259-5J	G 0 9 C 1/00	6 6 0 A
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 A
9/32				6 0 1 C
				6 0 1 E

審査請求 未請求 請求項の数22 O L (全 22 頁) 最終頁に続く

(21) 出願番号 特願平9-129972

(22) 出願日 平成9年(1997) 5月20日

(31) 優先権主張番号 特願平8-126751

(32) 優先日 平8(1996) 5月22日

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 松崎 なつめ

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 原田 俊治

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

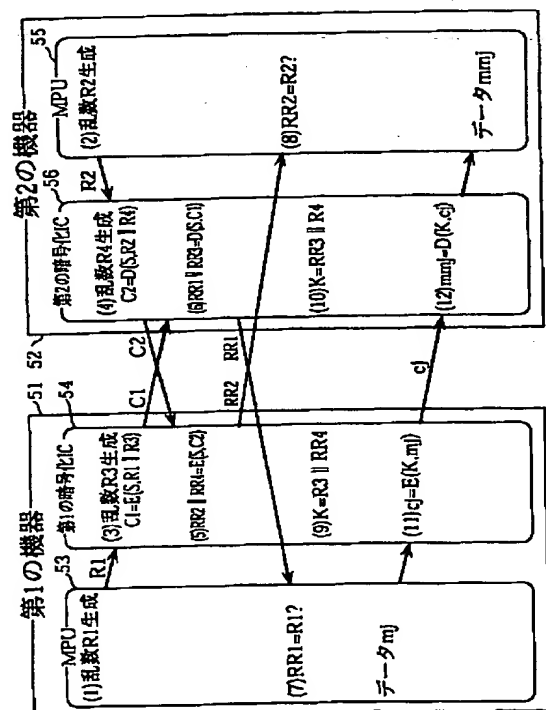
(74) 代理人 弁理士 中島 司朗

(54) 【発明の名称】 暗号化装置

(57) 【要約】

【課題】 規模の小さな暗号化 I C を備え、機器間通信の安全性を確保するための必要最小限の機能を有する暗号化装置を提供する。

【解決手段】 第1の機器51において、第1の暗号化 I C 54は、第2の機器を認証する過程(ステップ(1)、(3)、(6)、(7))で生成した乱数R3と、自らの正当性を第2の機器52に対して証明する過程(ステップ(2)、(4)、(5)、(8))で獲得した乱数RR4とを結合することで時変のデータ転送鍵を生成し(ステップ(9))、そのデータ転送鍵を用いてデジタル著作物を暗号化し、第2の機器52に転送する(ステップ(11))。



【特許請求の範囲】

【請求項 1】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、

前記データ転送鍵の共有化のための第 1 乱数を生成する第 1 乱数生成手段と、

前記第 1 乱数生成手段により生成された第 1 乱数を保持する第 1 乱数保持手段と、

前記第 1 乱数生成手段により生成された第 1 乱数を前記暗号通信の相手機器に送信する第 1 送信手段と、

前記第 1 乱数保持手段に保持された第 1 乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、

暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、

前記第 1 乱数生成手段、前記第 1 乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、1 個の IC 内の回路で実現され、

前記第 1 乱数保持手段は、前記 IC の外部からアクセスできない領域に前記第 1 乱数を保持することを特徴とする暗号化装置。

【請求項 2】 前記暗号化装置はさらに、前記第 1 乱数生成手段により生成された第 1 乱数を暗号化する第 1 暗号化手段を備え、

前記第 1 暗号化手段は、前記 IC 内の回路で実現され、前記第 1 送信手段は、前記第 1 暗号化手段で暗号化された第 1 乱数を前記相手機器に送信することを特徴とする請求項 1 記載の暗号化装置。

【請求項 3】 前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、

前記暗号化装置はさらに、

前記相手機器に送信するチャレンジデータ用の第 2 乱数を生成する第 2 乱数生成手段と、

前記チャレンジデータに対して前記相手機器から返信されてきたレスポンスデータと前記第 2 乱数とが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段とを備え、

前記データ転送鍵生成手段は、前記認証がなされた場合に前記データ転送鍵を生成することを特徴とする請求項 2 記載の暗号化装置。

【請求項 4】 前記第 2 乱数生成手段及び前記認証手段は、前記 IC 外の回路で実現されていることを特徴とする請求項 3 記載の暗号化装置。

【請求項 5】 前記暗号化装置はさらに、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、

復号化された結合データをレスポンスデータに相当する第 1 分離データと残る第 2 分離データとに分離する分離

手段と、

前記第 1 分離データを前記相手機器に返信する第 2 送信手段とを備え、

前記第 1 暗号化手段は、前記第 1 乱数と前記第 2 乱数とを結合し、その結果得られた結合データを暗号化し、

前記データ転送鍵生成手段は、前記第 1 乱数と前記第 2 分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段及び前記分離手段は、前記 IC 内の回路で実現されていることを特徴とする請求項 4 記載の暗号化装置。

【請求項 6】 前記暗号化装置はさらに、

前記第 2 乱数をチャレンジデータとして前記相手機器に送信する第 2 送信手段と、

前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、

復号化された結合データをレスポンスデータに相当する第 1 分離データと残る第 2 分離データとに分離する分離手段とを備え、

前記認証手段は、前記第 1 分離データを前記相手機器から返信されてきたレスポンスデータとして前記判断及び認証をし、

前記第 1 暗号化手段は、前記相手機器から送信されてきたチャレンジデータと前記第 1 乱数とを結合し、その結果得られた結合データを暗号化し、

前記データ転送鍵生成手段は、前記第 1 乱数と前記第 2 分離データとを結合することにより、前記データ転送鍵を生成し、

前記復号化手段及び前記分離手段は、前記 IC 内の回路で実現されていることを特徴とする請求項 4 記載の暗号化装置。

【請求項 7】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第 1 暗号化手段及び前記復号化手段の少なくとも 1 つのものと同一であることを特徴とする請求項 5 又は 6 記載の暗号化装置。

【請求項 8】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第 1 暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であることを特徴とする請求項 5 又は 6 記載の暗号化装置。

【請求項 9】 前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化することを特徴とする請求項 8 記載の暗号化装置。

【請求項 10】 前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうことを特徴とする請求項 9 記載の暗号化装置。

【請求項 11】 前記第 1 暗号化手段での暗号と前記復号化手段での復号化とは、同一の変換アルゴリズムであ

10

20

30

40

50

ることを特徴とする請求項 10 記載の暗号化装置。

【請求項 12】 前記第 1 暗号化手段及び前記復号化手段は、予め前記 IC 内に保持された鍵データを用いて前記暗号化及び復号化を行い、

その鍵データの一部は、前記 IC 内のマスク ROM 領域に格納され、残る一部は、前記 IC 内の追記 ROM 領域に格納されていることを特徴とする請求項 11 記載の暗号化装置。

【請求項 13】 前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記チャレンジデータに対して前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第 1 分離データと残る第 2 分離データとに分離する分離手段と、前記第 1 乱数と前記第 1 分離データとが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段と、前記認証がなされた場合に前記第 2 分離データを暗号化する第 2 暗号化手段と、暗号化された前記第 2 分離データをレスポンスデータとして前記相手機器に返信する第 2 送信手段とを備え、前記データ転送鍵生成手段は、前記第 1 乱数と前記第 2 分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段、前記分離手段及び前記第 2 暗号化手段は、前記 IC 内の回路で実現されていることを特徴とする請求項 2 記載の暗号化装置。

【請求項 14】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第 1 暗号化手段、前記第 2 暗号化手段及び前記復号化手段の少なくとも 1 つのものと同一であることを特徴とする請求項 13 記載の暗号化装置。

【請求項 15】 前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第 1 暗号化手段、前記第 2 暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であることを特徴とする請求項 13 記載の暗号化装置。

【請求項 16】 前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化することを特徴とする請求項 15 記載の暗号化装置。

【請求項 17】 前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうことを特徴とする請求項 16 記載の暗号化装置。

【請求項 18】 前記第 1 暗号化手段及び前記第 2 暗号

化手段での暗号化と前記復号化手段での復号化とは、いずれも同一の変換アルゴリズムであることを特徴とする請求項 17 記載の暗号化装置。

【請求項 19】 前記第 1 暗号化手段、前記第 2 暗号化手段及び前記復号化手段は、予め前記 IC 内に保持された鍵データを用いて前記暗号化及び復号化を行い、その鍵データの一部は、前記 IC 内のマスク ROM 領域に格納され、残る一部は、前記 IC 内の追記 ROM 領域に格納されていることを特徴とする請求項 18 記載の暗号化装置。

【請求項 20】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞ

れ、チャレンジデータ用の第 1 乱数を生成する第 1 乱数生成手段と、

前記データ転送鍵用の第 2 乱数を生成する第 2 乱数生成手段と、

前記第 1 乱数と前記第 2 乱数を結合する結合手段と、

前記結合データを暗号化する暗号化手段と、

暗号化された前記結合データを前記相手機器に送信する第 1 送信手段と、

前記相手機器の第 1 送信手段から送信された暗号化された結合データを受信する第 1 受信手段と、

受信した前記結合データを復号化する復号化手段と、

復号化された前記結合データをレスポンスデータに相当する第 1 分離データと前記データ転送鍵用の第 2 分離データに分離する分離手段と、

前記第 1 分離データをレスポンスデータとして前記相手機器に返信する第 2 送信手段と、

前記相手機器の第 2 送信手段から返信された第 1 分離データを受信する第 2 受信手段と、

受信した前記第 1 分離データと前記第 1 乱数とを比較

し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、

前記第 2 乱数と前記第 2 分離データとを結合すること

で、前記データ転送鍵を生成するデータ転送鍵生成手段と、

前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする暗号化装置。

【請求項 21】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、

それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞ

れ、
 チャレンジデータ用の第1乱数を生成する第1乱数生成手段と、
 前記第1乱数を前記相手機器に送信する第1送信手段と、
 前記相手機器の第1送信手段から送信された第1乱数を受信する第1受信手段と、
 前記データ転送鍵用の第2乱数を生成する第2乱数生成手段と、
 受信した前記第1乱数と前記第2乱数を結合する結合手段と、
 前記結合データを暗号化する暗号化手段と、
 暗号化された前記結合データを前記相手機器に返信する第2送信手段と、
 前記相手機器の第2送信手段から送信された暗号化結合データを受信する第2受信手段と、
 受信した前記結合データを復号化する復号化手段と、
 復号化された前記結合データをレスポンスデータに相当する第1分離データと前記データ転送鍵用の第2分離データに分離する分離手段と、
 前記第1分離データと前記第1乱数生成手段で生成された前記第1乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、
 前記第2乱数と前記第2分離データとを結合することで、前記データ転送鍵を生成するデータ転送鍵生成手段と、
 前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする暗号化装置。
 【請求項22】 データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、
 それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、
 前記送信機は、
 第1乱数を生成する第1乱数生成手段と、
 前記第1乱数を暗号化する第1暗号化手段と、
 暗号化された前記第1乱数を受信機に送信する第1送信手段とを備え、
 前記受信機は、
 暗号化された前記第1乱数を受信する第1受信手段と、
 受信した前記第1乱数を復号化する第1復号化手段と、
 第2乱数を生成する第2乱数生成手段と、
 前記第1乱数と前記第2乱数を結合することで、結合データを生成する第1結合手段と、
 前記結合データを暗号化する第2暗号化手段と、
 暗号化された前記結合データを送信機に送信する第2送信手段とを備え、
 前記送信機はさらに、

暗号化された前記結合データを受信する第2受信手段と、
 受信した前記結合データを復号化する第2復号化手段と、
 復号化された前記結合データを前記第1乱数に相当する第1分離データと前記第2乱数に相当する第2分離データとに分離する分離手段と、
 前記第1乱数と前記第1分離データとを比較し、一致している場合に前記受信機を正当な機器と認証する第1比較手段と、
 前記認証がなされた場合に前記第2分離データを暗号化する第3暗号化手段と、
 暗号化された前記第2分離データを前記受信機に送信する第3送信手段と前記第1乱数生成手段で生成された第1乱数と前記分離手段で得られた第2分離データとを結合することで、前記データ転送鍵を生成する第1データ転送鍵生成手段とを備え、
 前記受信機はさらに、
 暗号化された前記第2分離データを受信する第3受信手段と、
 受信した前記第2分離データを復号化する第3復号化手段と、
 復号化された前記第2分離データと前記第2乱数とを比較し、一致している場合に前記送信機を正当な機器と認証する第2比較手段と、
 前記認証がなされた場合に前記第1復号化手段で得られた前記第1乱数と前記第2乱数生成手段で生成された第2乱数とを結合することで、前記データ転送鍵を生成する第2データ転送鍵生成手段とを備え、
 前記送信機はさらに、
 前記第1データ転送鍵生成手段で生成されたデータ転送鍵を用いて転送データを暗号化する第4暗号化手段と、
 暗号化された転送データを前記受信機に送信する第4送信手段とを備え、
 前記受信機はさらに、
 暗号化された前記転送データを前記送信機から受信する第4受信手段と、
 前記第2データ転送鍵生成手段で生成されたデータ転送鍵を用いて転送データを復号化する第4復号化手段とを備えることを特徴とする暗号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、秘密鍵を共有して暗号通信を行なう通信機器に備えられる暗号化装置に関し、特に、小さい回路規模で実現することができる暗号化装置に関する。

【0002】

【従来の技術】通信路を介して通信されているデータが通信路上で不正にコピーされたり改変されることを防ぐことが必要となる場合が数多くある。例えば、映画など

の著作物がデジタル化されさらに情報圧縮され、さらに光ディスク上にデジタル記録されており、これが光ディスク再生装置により電気情報として取り出され、取り出されたデジタル情報が情報伸長装置により伸長され、映像音響再生装置により再生されるような場合である。

【0003】ここで光ディスク再生装置と情報伸長装置は別々の機器として分離しており、その間がデジタル通信路によりデータ通信される場合、この通信データが著作権者の許可なくデジタル情報記録装置により記録され、さらにデジタル情報複製装置により複製されるものであれば、その映画の著作物が不正に複製されることになり、著作権の侵害が起こる。従って通信路を介して通信されているデータが通信路上で不正にコピーされることを防がなければならない。機器内の回路や部品の仕様が一般には公開されないのに対し、データ通信のための電気的特性や信号形式は一般に公開される場合が多いので通信路におけるデータの不正コピーやそれに引き続くデータの改変が大きな問題になる。

【0004】このような不正行為を排除して安全な通信を確保するための技術については従来より様々なものが知られている。最も代表的なものは相手認証技術を用いるものである。これは基本的にはデータを送出する側が受信する側の正当性を認証し、正当な受信者であることが確認できたときのみデータを送信することで、デジタル著作物が不正な機器に受信されることを防止するものである。

【0005】なお、この場合の受信者のように自らの正当性を証明する側を証明者と呼び、またこの場合の送信者のように相手の正当性を確認する側を認証者と呼ぶ。また、前述の光ディスク記録再生に関わる機器のような場合には、特定の機器の間で認証が成功するか否かということよりも、それら機器が光ディスク関連機器の業界によって定められた規格に準拠したものであるか否かが問題となる。従ってこのような場合には、「正当性」とは「所定の規格に準拠すること」を意味する。

(第1の従来技術) 第1の具体的な従来技術として、国際標準規格ISO/IEC9798-2に記載される暗号技術を用いた一方向認証方法がある。

【0006】この認証方法は証明者が認証鍵と呼ばれる秘密のデータを持つことを、その鍵自身を知らせることなく認証者に対して証明することを基本としている。そのためにまず認証者があるデータを選びこれを証明者に対して投げかける。この行為をチャレンジ、投げかけたデータをチャレンジデータと呼ぶ。これに対して証明者は、予め所有していた暗号変換と認証鍵を用いて前記チャレンジデータを暗号化する。そして、暗号化したデータを認証者に返す。この行為をレスポンス、そのデータをレスポンスデータと呼ぶ。

【0007】このレスポンスデータを受信した認証者

は、証明者が所有している暗号変換の逆変換である復号変換と認証鍵を共有しており、証明者から返信されてきたレスポンスデータをその認証鍵と復号変換を用いて復号化する。この結果が前記チャレンジデータと一致すれば受信者は正規の認証鍵を持つものと判断し、証明者の正当性を認証する。一方向認証とは一方の側がその正当性を他方に証明することを意味する。

【0008】ここで、暗号変換Tとは、鍵データSにより定まる平文集合から暗号文集合への写像である。平文をXとしたとき暗号文を $T(S, X)$ と書く。同じ鍵データSにより定まる暗号文集合から平文集合への写像である逆変換 $TINV$ との間には、

$$TINV(S, T(S, X)) = X$$

の関係がある。これは平文Xを暗号変換し、これを逆変換すると元に戻ることを意味している。暗号変換の逆変換を復号変換と呼ぶ。暗号変換であるためには鍵Sの知識がないときに暗号文 $T(S, X)$ から平文Xを求めるのが困難であることが必要である。なお、慣例により暗号変換を $E(S, \quad)$ 、復号変換を $D(S, \quad)$ と記す。

【0009】図11は、前記規格に記載されている認証方法の一例を示す図である。図11では、第1の機器11から第2の機器12にデジタル著作物 m_j を転送する場合が示されている。ここでは、第1の機器11が第2の機器12の正当性を確認する。以下この従来の一方向認証方法の動作を同図に示されたステップ番号に従って説明する。

【0010】(1) 第1の機器11は、乱数 $R1$ を生成する。そしてこれをチャレンジデータとして通信路を介して第2の機器12に送信する。

(2) 第2の機器12はこの乱数を受けとると、第2の機器12に格納されている秘密の認証鍵 S を暗号鍵としてこの乱数を暗号化する。そしてその結果 $C1$ をレスポンスデータとして通信路を介して第1の機器11に送信する。

【0011】(3) 第1の機器11はこのレスポンスデータを受け取ると、第1の機器11に格納されている認証鍵 S を復号鍵としてこのレスポンスデータ $C1$ を復号化する。

(4) 第1の機器11は、復号の結果 $RR1$ を第1の機器11内に一時保管されている乱数 $R1$ と比較する。これが一致すれば第1の機器11は第2の機器12機器が同じ認証鍵 S を保有するものと考え、通信相手が正当なものであると認証する。一方、一致しなければ通信相手が正当なものではないものと判断して処理を中断する。

【0012】(5) 第1の機器11は第2の機器12を正当なものと認証した後、デジタル著作物を通信路を介して第2の機器12に送信する。もしも、第2の機器12の代わりに認証鍵 S を有さない第3の機器が通信路に接続されている場合には、その第3の機器は上記ステップ

(2)で正しい値のデータC1を作成することができず、結果としてステップ(3)で復号の結果RR1が前記R1と一致しないため、ステップ(4)において第1の機器11はデジタル著作物をその第3の機器に伝送しない。

【0013】なお、第1の機器11と第2の機器12の間でいつも同じチャレンジデータとレスポンスデータが用いられるならば、そのことを知った不正な第3の機器が第2の機器12になりすますことが考えられる。これを避けるために第1の機器11からは毎回異なるチャレンジデータ(乱数)を送っている。

(第2の従来技術)ところで、上記第1の従来技術では、例えば認証の後、ハードディスク装置に記憶されている偽りのデータを正規の認証鍵を有する第2の機器12に対して不正に送出することも可能である。この問題を解決するため、第1の機器11が第2の機器12の正当性を確認すると同時に、第2の機器12も第1の機器11の正当性を確認することが必要となる。

【0014】また、双方の機器が認証した後にデジタル著作物を通信路を介して第2の機器12に伝送している最中に、この通信路上のデータを抜きとり、これを例えばハードディスク装置に記憶することが考えられる。もちろんこのためには通信路上の信号の電気的特性やデータ形式などの知識が必要であるが、それらの知識は一般に特に秘密にされている情報ではないので、そのデジタル著作物の抜きとりは技術的に十分に可能である。そのため、認証だけでは不十分であり、認証が成功した後に、各機器間でランダムに生成した新たな鍵を共有し、その鍵を用いてデジタル著作物を暗号化して転送する暗号通信をすることが必要になる。なお、デジタル著作物等の転送すべきデータを暗号化するための秘密鍵を、以下、「データ転送鍵」と呼ぶ。

【0015】以下、上記第1の従来技術である一方向認証を拡張し、双方向認証とデータ転送鍵の共有化と暗号通信とを行なう第2の従来技術を説明する。図12は、この双方向認証を実現する装置の一例を示す。図12には、第1の機器21から第2の機器22にデジタル著作物mjを暗号化した後に転送する場合が示されている。

【0016】以下この従来の双方向認証とデータ転送鍵の共有化の動作を同図に示されたステップ番号に従って説明する。

(1) 第1の機器21は乱数R1を生成する。これは第1のチャレンジデータとしての意味を持つ。そしてこれを通信路を介して第2の機器22に送信する。ここで乱数R2は第2の機器22から第1の機器21への第2のチャレンジデータとしての意味を持つ。つまり、暗号文C1は第1のチャレンジデータに対するレスポンスデータと第2のチャレンジデータの両方の意味を持つ。

【0017】(2) 第2の機器22は乱数R2を生成し、それと第1の機器21から受けとった乱数R1とを結合することで結合データR1||R2を作成する。ここで記

号”||”は双方のデータを桁方向に並べて結合することを示す。そして第2の機器22の認証鍵Sを暗号鍵として、この結合データR1||R2を暗号化し、その暗号文C1を第1の機器21に送信する。

【0018】(3) 第1の機器21は、第2の機器22から受信した暗号文C1を認証鍵Sを復号鍵として復号化し、その結果の上位を分離データRR1、下位を分離データRR2とする。

(4) 第1の機器21では、この分離データRR1を第1の機器21に一時記憶されている乱数R1と比較する。これが一致すれば通信相手が認証鍵Sを持っている正当な機器であると認証する。もしも一致しなければここで認証処理を中断する。

【0019】(5) 第1の機器21は、乱数Kを発生しこれをデータ転送鍵Kとして設定する。そして前記獲得した分離データRR2とこのデータ転送鍵Kを結合した結合データRR2||Kを第1の機器21の認証鍵Sで暗号化して、その暗号文C2を第2の機器22に送信する。

(6) 第2の機器22は、第1の機器21から受信した暗号文C2を認証鍵Sを用いて復号化し、その上位を分離データRRR2、下位を分離データKKとする。

【0020】(7) 第2の機器22は、この分離データRRR2を第2の機器22に一時記憶されている乱数R2と比較する。これが一致すれば通信相手が認証鍵Sを持っている正当な機器であると認証する。もしも一致しなければ、ここで認証処理を中断する。一方、復号化した分離データKKをデータ転送鍵KKとして設定する。

【0021】(8) 第1の機器21は、前記データ転送鍵Kを用いてデジタル著作物を暗号化し、通信路を介して第2の機器22に送信する。

(9) 第2の機器22ではこれを前記データ転送鍵KKを用いて復号化し、もとのデジタル著作物を獲得する。ここで、もしも第1の機器21が正規の認証鍵Sを有し、第2の機器22が正規の認証鍵を有していない場合には、ステップ(4)で第1の機器21は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。また第1の機器21が正規の認証鍵を有しておらず、第2の機器22は正規の認証鍵を有している場合には、ステップ(7)において第2の機器22は通信相手が正規の認証鍵を有していないものと判断し、認証処理を中断できる。このようにしてデジタル著作物が不正な機器に流出することを防止すると同時に不正な機器から正当な機器に流入することも防止することができる。

【0022】さらに、第1の機器21も第2の機器22も正当な認証鍵を有している場合において前記認証処理が完了しステップ(8)においてデジタル著作物が通信路上を伝送されている際に、もし、そのデジタル著作物が電氣的にコピーされ、デジタル蓄積装置に蓄積された場合であっても、そのデジタル著作物は暗号化されているので、無意味なデジタルデータとなっており、元の

デジタル著作物は有効に保護される。

【0023】以上のように、暗号技術を用いた双方向認証が首尾よく行われるには、第1の機器21及び第2の機器22の内部に格納されている認証鍵が不正を行おうとするものに容易に分かることが必須の条件となる。また、チャレンジデータのための乱数の生成部やデータ転送鍵Kの生成部が外部からアクセス不可なこと、変更できないことが必要である。

【0024】それら構成要素の秘匿性を確保する最も効果的な方法は、上記の認証やデータ転送鍵の共有化及び暗号通信を行う部分をICとして実現する方法である。ICを解析するには一般に多大な労力がかかるので、認証鍵などが容易には解読されないからである。

【0025】

【発明が解決しようとする課題】ところが、上記の第2従来技術における第1の機器21をICで実現するためには、そのようなIC（以下、「暗号化IC」という。）は次の部分を備えることが必要である。

- ・乱数R1を生成する乱数生成部
- ・暗号文C1を復号化するための復号部
- ・認証鍵Sを格納する部分
- ・乱数R1と分離データRR1を比較するための比較部
- ・データ転送鍵Kを生成するための乱数生成部
- ・分離データRR2とデータ転送鍵Kを結合して暗号化するための暗号部
- ・データ転送鍵Kを格納する部分
- ・データ転送鍵Kを用いてデジタル著作物を暗号化する暗号部

第2の機器22についてもこれと同程度の規模のハードウェアが必要である。

【0026】このように、上記従来の認証方式をICで実現したのでは、2つの乱数生成部、2つの変換部（復号部と暗号部）非常に多くの機能を持たなければならないために、回路規模が大きくなり結局機器のコストアップにつながるという問題点を有する。また、上記第2従来技術ではデータを暗号化するためのデータ転送鍵Kは第1の機器21が生成しているが、相互認証が必要とされるのと同じ理由により、この鍵は双方の機器が生成した値を反映するほうが望ましい。

【0027】以上説明したように、機器間の回線を保護するためには、認証等の機能やそのための秘密の情報をICに封じ込めて実現する方法が効果的である。しかし、従来の方法において、相互認証の部分、データ転送鍵の共有化の部分及びデータ暗号化の部分をすべて1つのICで実現するのでは、そのICの規模は非常に大きくなってしまい、コストアップにつながる。

【0028】そこで、本発明は、規模の小さな暗号化ICを備え、機器間通信の安全性を確保するための必要最小限の機能を有する暗号化装置を提供することを第1の目的とする。ここで暗号化ICは次の機能を有する。

(1) 認証鍵を安全に格納する。その鍵は外部からのアクセスにより書き換え及び読み出しがなされない。

【0029】(2) データ転送鍵を安全に共有する。その鍵は外部からのアクセスにより書き換え及び読み出しがなされない。

(3) 但し、通信システムの安全性に関連しない部分を暗号化ICに備えないことにより、暗号化ICの規模を最小とする。また、本発明の第2の目的は、規模の小さな暗号化ICを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムを提供することである。

【0030】

【課題を解決するための手段】上記第1の目的を達成するために本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、前記データ転送鍵の共有化のための第1乱数を生成する第1乱数生成手段と、前記第1乱数生成手段により生成された第1乱数を保持する第1乱数保持手段と、前記第1乱数生成手段により生成された第1乱数を前記暗号通信の相手機器に送信する第1送信手段と、前記第1乱数保持手段に保持された第1乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、前記第1乱数生成手段、前記第1乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、1個のIC内の回路で実現され、前記第1乱数保持手段は、前記ICの外部からアクセスできない領域に前記第1乱数を保持することを特徴とする。

【0031】これにより、データ転送鍵の生成に直接関連する第1乱数は外部からアクセスできない暗号化ICの内部に保持されるので、時変のデータ転送鍵は各機器に安全に共有され、暗号通信が行われる。また、暗号化ICは、機器間通信の安全性を確保するための必要最小限の機能を持つので、小さな回路で実現することができる。

【0032】また、上記第2の目的を達成するために本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に相手機器が正当な機器であることを認証し合うものであり、それぞれ、チャレンジデータ用の第1乱数を生成する第1乱数生成手段と、前記データ転送鍵用の第2乱数を生成する第2乱数生成手段と、前記第1乱数と前記第2乱数を結合する結合手段と、前記結合データを暗号化する暗号化手段と、暗号化された前記結合データを前記相手機器に送信する第1送信手段と、前記相手機器の第1送信手段から送信された暗号化された結合データを受信する第1受信手段と、受信した前記結合データを復号化する復号化手段と、復号化された前記結合

データをレスポンスデータに相当する第1分離データと前記データ転送鍵用の第2分離データに分離する分離手段と、前記第1分離データをレスポンスデータとして前記相手機器に返信する第2送信手段と、前記相手機器の第2送信手段から返信された第1分離データを受信する第2受信手段と、受信した前記第1分離データと前記第1乱数とを比較し、一致している場合に前記相手機器を正当な機器と認証する比較手段と、前記第2乱数と前記第2分離データとを結合することで、前記データ転送鍵を生成するデータ転送鍵生成手段と、前記認証がなされた場合に、生成された前記データ転送鍵を用いて前記相手機器と暗号通信を行なう暗号通信手段とを備えることを特徴とする。

【0033】これにより、送信機及び受信機間で相互認証が行われると共にデータ転送鍵が生成されること、データ転送鍵の生成に直接関連する乱数はそのままでは送受信されないこと、及び、データ転送鍵の生成に直接関連する2つの乱数はそれぞれ送信機及び受信機から提供されたものであることから、規模の小さな暗号化ICを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムが実現される。

【0034】

【発明の実施の形態】

(実施の形態1) 図1は、本発明に係る暗号化装置を備えた第1の機器と第2の機器間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行う実施の形態1における処理シーケンスを示す図である。

【0035】図1では、第1の機器51から第2の機器52にデジタル著作物mjを転送する場合が示されている。なお、図1には、各機器51、52が備える暗号化装置だけが示されており、暗号化装置と直接に関連しない他の構成要素(送受信部やデジタル著作物の処理系等)は省略されている。第1の機器51に備えられた本発明に係る暗号化装置は、大きく分けてMPU53と第1の暗号化IC54とから構成される。

【0036】MPU53は、この暗号化装置に固有の制御プログラムを保持するROMとその制御プログラムを実行する汎用マイクロプロセッサとRAM等からなり、データ転送鍵の共有化に直接的には関与しない処理(図中のステップ(1)、(7))を行なう。第1の暗号化IC54は、1チップの半導体ICであり、データ転送鍵の共有化に直接的に関与する処理(図中のステップ(3)、(5)、(9)、(11))を行なう。

【0037】同様に、第2の機器52に備えられた本発明に係る暗号化装置も、大きく分けてMPU55と第2の暗号化IC56とから構成される。MPU55は、この暗号化装置に固有の制御プログラムを保持するROMとその制御プログラムを実行する汎用マイクロプロセッサとRAM等からなり、データ転送鍵の共有化に直接的には関与しない処理(図中のステップ(2)、(8))を行な

う。

【0038】第2の暗号化IC56は、1チップの半導体ICであり、データ転送鍵の共有化に直接的に関与する処理(図中のステップ(4)、(6)、(10)、(12))を行なう。なお、この実施の形態においては、データ暗号化規格(DES:Data Encryption Standard)に準拠した64ビットブロック暗号アルゴリズムEとその逆変換アルゴリズムDを用いている。以降では暗号アルゴリズムEを用いる変換を「暗号化」、逆変換アルゴリズムDを用いる変換を「復号化」と称する。

【0039】また、第1の暗号化IC54は暗号アルゴリズムEだけを、第2の暗号化IC56は逆変換アルゴリズムDだけを備える。これは、各暗号化IC54、56の規模を削減することと、安全性のためである。以下、図1に示されたステップ番号に従って、実施の形態1における暗号化装置の動作を説明する。

【0040】(1) 第1の機器51のMPU53において乱数R1(32ビット)を生成して、記憶するとともに第1の暗号化IC54に渡す。

(2) ステップ(1)と同様に、第2の機器52のMPU55において乱数R2(32ビット)を生成して、記憶するとともに第2の暗号化IC56に送信する。

【0041】(3) 第1の暗号化IC54において、乱数R3(32ビット)を生成、外部よりアクセスできない領域に格納する。そして、前記MPUで生成した乱数R1と前記乱数R3を結合してE関数で暗号化する。ここで、記号“||”は2つの乱数を桁方向に結合して64ビット(乱数R1を上位32ビット、乱数R3を下位32ビット)とすることを示している。また、暗号化には第1の暗号化IC54及び第2の暗号化IC56で予め共通に保持している秘密の認証鍵Sを用いる。第1の暗号化IC54は、第1の機器51の送信部(図では示していない)を介して上記暗号結果C1を第2の機器52に送信する。

【0042】(4) ステップ(3)と同様に、第2の暗号化IC56において、乱数R4(32ビット)を生成して、外部よりアクセスできない領域に格納する。前記MPUで生成した乱数R2と前記乱数R4を結合して逆変換アルゴリズムDで復号化する。復号には前記認証鍵Sを用いる。第2の暗号化IC56は、第2の機器52の送信部(図では示していない)を介して復号結果C2(64ビット)を第1の機器51に送信する。

【0043】(5) 第1の暗号化IC54において、前記第2の機器52から受信した復号文C2を前記E関数を用いて前記認証鍵Sで暗号化する。そして、得られた64ビットをその上位32ビットである分離データRR2と下位32ビットである分離データRR4に分離する。さらに、分離データRR2は第1の機器51の送信部を介して第2の機器52に送信し、一方、分離データRR4は外に出さずに第1の暗号化IC54内の外部からア

アクセスできない領域に格納する。

【0044】なお、第1の暗号化IC54及び第2の暗号化IC56が互いに正規なものであり同じ認証鍵Sを保持している場合には、前記分離データRR2は前記第2の機器52のMPU55が生成した乱数R2と一致し、前記分離データRR4は前記第2の暗号化IC56が内部に格納している乱数R4と一致する。

(6) ステップ(5)と同様に、第2の暗号化IC56において、前記第1の暗号化IC54から受信した暗号文C1を前記逆変換アルゴリズムDを用いて前記認証鍵Sで復号化する。そして、得られた64ビットをその上位32ビットである分離データRR1と下位32ビットである分離データRR3に分離する。さらに、分離データRR1は第2の機器52の送信部を介して第1の機器51に送信し、一方、分離データRR3は外に出さずに第2の暗号化IC56内の外部からアクセスできない領域に格納する。

【0045】なお、第1の暗号化IC54及び第2の暗号化IC56が互いに正規なものであり同じ認証鍵Sを保持している場合には、前記分離データRR1は前記乱数R1と一致し、前記分離データRR3は前記乱数R3と一致する。

(7) 第1の機器51のMPU53において前記ステップ(1)で記憶していた乱数R1と前記第2の機器52から受信した分離データRR1とを比較し、一致している場合には、第2の暗号化IC56及びそれを備えた第2の機器52を正当な機器と認証する。

【0046】(8) ステップ(7)と同様に、第2の機器52のMPU55において前記ステップ(2)で記憶していた乱数R2と前記第2の機器52から受信した分離データRR2とを比較し、一致している場合には、第1の暗号化IC54及びそれを備えた第1の機器51を正当な機器と認証する。

(9) 第1の暗号化IC54において、前記ステップ(3)で記憶しておいた乱数R3と前記分離データRR4を結合することでデータ転送鍵Kを作成する。ここでは、乱数R3を上位の32ビット、分離データRR4を下位の32ビットとするデータ転送鍵K(64ビット)を生成する。なお、このデータ転送鍵Kは、2つの乱数の結合であるので、時変、即ち、新たにランダムに生成された鍵と言える。

【0047】(10) ステップ(9)と同様に、第2の暗号化IC56において、前記分離データRR3と前記ステップ(4)で記憶しておいた乱数R4を結合することでデータ転送鍵Kを生成する。ここでは、上記分離データRR3を上位の32ビット、上記ステップ(4)で記憶しておいた乱数R4を下位の32ビットとするデータ転送鍵K(64ビット)を生成する。このデータ転送鍵も時変の鍵である。

【0048】なお、ステップ(7)及びステップ(8)での相

互の認証が成功した場合には、ステップ(3)で生成された乱数R3とステップ(6)で得られた分離データRR3とは一致し、ステップ(4)で生成された乱数R4とステップ(5)で得られた分離データRR4とは一致することになるので、結果的に、ステップ(9)及びステップ(10)それぞれで生成されるデータ転送鍵Kは一致することになる。

【0049】(11) 第1の機器51の第1の暗号化IC54において、MPU53から送られてくるブロック化されたデジタル著作物mj(64ビット)を上記ステップ(9)で得られたデータ転送鍵Kを用いて暗号化し、得られた暗号文Cjを第2の機器52に送信する処理を、転送すべき全てのデジタル著作物を送信し終えるまで繰り返す。

【0050】(12) ステップ(11)に対応して、第2の機器52の第2の暗号化IC56において、第1の機器51が送信した暗号化された上記デジタル著作物Cj(64ビット)を受信し、上記ステップ(10)で得られたデータ転送鍵Kを用いて復号化し、得られたデジタル著作物mmjをMPU55に送る。この復号化は上記デジタル著作物Cjが第1の機器51から送信されてくる限り繰り返す。

【0051】このようにして、実施の形態1の暗号化装置により、第1の機器51と第2の機器52間で相互認証とデータ転送鍵Kの共有化とデータの暗号通信とが行われる。以上の説明から明らかなように、上記実施の形態1の暗号化装置は、以下の特徴を有する。

【0052】第1の特徴は、データ転送鍵Kは暗号化ICの内部に安全に保護されていることである。具体的には、第1の機器51が備える暗号化装置であれば、データ転送鍵Kを生成するために直接的に用いられた2つのデータ、即ち、乱数R3と分離データRR4は以下の条件を満たす。

・乱数R3は、第1の暗号化IC54の内部で生成され、外部に出力されておらず、かつ、外部から読めない領域に保持されている。

【0053】・分離データRR4は、第1の暗号化IC54の内部で生成(分離生成)され、外部に出力されておらず、かつ、外部から読めない領域に保持されている。これらのことにより、データ転送鍵Kは暗号化IC内に保護されるので、暗号アルゴリズムE及び逆変換アルゴリズムDとして公開されているものを採用したとしても、第1の機器51及び第2の機器52間における暗号通信の安全性は保証される。

【0054】第2の特徴は、暗号化IC内に納められる回路は、必要最低限のものに留められていることである。具体的には、第1の機器51が備える暗号化装置であれば、以下の処理は、第1の暗号化IC54の外の回路、即ち、MPU53によって実現されている。

・乱数R1の生成

・乱数R1と分離データRR1との比較

つまり、第1の暗号化IC54の回路規模が不必要に大きくならないように配慮されている。これら2つの処理は、相手機器の認証に関するものであり、データ転送鍵Kの生成に直接的には関与していない。従って、たとえば、これら処理がIC外で実現されていることを利用して不正をしようとしても、第1の機器51に利益をもたらすような不正をはたらくことは不可能である。なお、第2の機器52からのチャレンジデータC2に対するレスポンスデータRR2の作成は暗号化IC内で行っている。

【0055】図2は、第1の暗号化IC54のハードウェア構成を示すブロック図である。第2の暗号化IC56も同程度のハードウェア規模で実現できる。外部I/F部61は、この第1の暗号化IC54の内部回路に外部からアクセスするための唯一の入出力ポートである。乱数生成部60は、32ビットの乱数R3を生成する。

【0056】乱数格納部62は、乱数生成部60で生成された乱数R3を保持する記憶回路である。結合部63は、乱数格納部62に格納された乱数R3を下位32ビットとし、外部I/F部61を介して入力された32ビットのデータR1を上位32ビットとして結合する。

【0057】認証鍵S格納部64は、予め与えられた認証鍵Sを保持する記憶回路である。スイッチ65、66は、それぞれ64ビット幅の3入力1出力マルチプレクサ、64ビット幅の2入力1出力マルチプレクサである。E関数67は、暗号アルゴリズムEに基づく暗号化回路である。スイッチ68は、64ビット幅の1入力3出力デマルチプレクサである。

【0058】分離部69は、スイッチ68から出力された64ビットデータを上位32ビットRR2と下位32ビットRR4に分離する。データ転送鍵K生成部59は、乱数格納部62に格納された乱数R3を上位32ビットとし、分離部69で分離された分離データRR4を下位32ビットとして結合することで、データ転送鍵Kを生成する。

【0059】データ転送鍵K格納部70は、データ転送鍵K生成部59で生成されたデータ転送鍵Kを保持する記憶回路である。次に、この図2に示された各構成要素が図1に示された各ステップにおいていかに動作するかを示す。図1のステップ(3)においては、乱数生成部60は乱数R3を生成して乱数格納部62に格納し、結合部63はその乱数R3と外部I/F部61を介して入力される乱数R1とを結合し、スイッチ65を介してE関数67に送る。E関数67は、認証鍵S格納部64からスイッチ66を介して認証鍵Sを受け取り、それを用いて結合部63から出力された結合データR1||R3を暗号化し、その結果C1をスイッチ68及び外部I/F部61を介して第2の機器52に出力する。

【0060】図1のステップ(5)及び(9)においては、外

部I/F部61を介して入力される復号文C2はスイッチ65を経てE関数に入力される。E関数67は、認証鍵S格納部64から認証鍵Sを受け取り、それを用いて復号文C2を暗号化し、スイッチ68を介して分離部69に送る。分離部69は、それを分離データRR2と分離データRR4に分離し、分離データRR2は外部I/F部61を介して外部に出力し、分離データRR4はデータ転送鍵K生成部59に送る。データ転送鍵K生成部59は、乱数格納部62に格納されていた乱数R3と分離部69から送られてきた分離データRR4とを結合することでデータ転送鍵Kを生成した後に、データ転送鍵K格納部70に格納する。

【0061】図1のステップ(11)においては、E関数67は、外部I/F部61及びスイッチ65を介して入力されるデジタル著作物mjをデータ転送鍵K格納部70に格納されたデータ転送鍵Kを用いて暗号化し、その結果Cjをスイッチ68及び外部I/F部61を介して第2の機器52に出力する。なお、実施の形態1では、乱数や暗号文等の具体的なビット長やデータ構成を示したが、本発明はそれらに限定されるものではない。例えば、上記ステップ(5)において32ビットの乱数R1とR2を結合して64ビットとし、これを64ビット暗号関数Eに入力して64ビットの暗号文C1を求めている。この部分は、例えば、各乱数を64ビットとし、暗号関数Eによる暗号化を2回繰り返すことで128ビットの暗号文C1を生成する方式としてもよい。ただしこの場合には暗号文C1から乱数R1に関する部分とR2に関する部分が容易に切り離せないことが必要である。その方法の1つとしてはCBCモードのように連鎖を伴う暗号の方法がある。CBCモードについては、池野信一、小山謙二共著「現代暗号理論」電子通信学会1986年のp70に詳しい。

【0062】また、実施の形態1では第1の暗号化IC54は暗号関数Eだけを、第2の暗号化IC56はその逆関数Dだけを備えることにより、ハードウェア規模を削減しているが、そのこと自体は、上述したように本発明の本質ではない。つまり、それら暗号化IC54、56に許容される回路規模や暗号化アルゴリズムの種類等との関連において決定すればよい事項であり、例えば、それぞれが暗号アルゴリズムEと逆変換アルゴリズムDの両方を所有し、乱数の暗号化に暗号アルゴリズムEを、相手機器から送付された情報の復号に逆変換アルゴリズムDを用いてもよい。本発明は、少なくともデータ転送鍵Kの生成に直接関わる構成要素をIC化することで秘密通信の安全性を確保している点に特徴があるからである。

【0063】また、実施の形態1において、例えば、ステップ(1)での乱数R1の生成を第1の暗号化IC54内で行ってもよい。このことにより、第1の暗号化IC54を暗号解読器として用いる可能性をなくし、より安

全な暗号化装置とすることができる。つまり、実施の形態 1 では、乱数 R1 は第 1 の暗号化 IC54 の外部で生成され、この乱数 R1 に基づいて第 1 の暗号化 IC54 は暗号文 C1 を出力する。この暗号文 C1 は、第 1 の暗号化 IC54 の内部で生成された乱数 R3 の影響を受けているが、もし乱数 R3 が十分にランダムな値でない場合には、第 1 の暗号化 IC54 を暗号解読器として悪用することが可能になってしまう。従って、乱数 R1 の生成を第 1 の暗号化 IC54 内で行うことで、以上述べた攻撃の可能性がなくなり、この暗号化装置はより安全なものになる。

(実施の形態 2) 次に、図 1 に示された実施の形態 1 でのステップの変形例として、実施の形態 2 を示す。その目的や効果は実施の形態 1 と同じである。またハードウェア規模としても図 2 に示された実施の形態 1 と同程度である。実施の形態 1 ではチャレンジデータを暗号化しないでレスポンスデータを暗号化して通信したが、実施の形態 2 ではチャレンジデータを暗号化しレスポンスデータを暗号化しないで通信する。実施の形態 1 と相違する点を中心に説明する。

【0064】図 3 は、本発明に係る暗号化装置を備えた第 1 の機器 71 と第 2 の機器 72 間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行う実施の形態 2 における処理シーケンスを示す図である。図 3 では、第 1 の機器 71 から第 2 の機器 72 にデジタル著作物 m_j を転送する場合が示されている。

【0065】MPU73、第 1 の暗号化 IC74、MPU75 及び第 2 の暗号化 IC76 は、実施の形態 1 における MPU53、第 1 の暗号化 IC54、MPU55 及び第 2 の暗号化 IC56 に対応し、処理手順の相違を除いて、ハードウェア構成等については実施の形態 1 の場合と同様である。以下、図 3 に示されたステップ番号に従って、実施の形態 2 における暗号化装置の動作を説明する。

【0066】(1) 第 1 の機器 71 の MPU73 において乱数 R1 (32 ビット) を生成して、記憶するとともに第 1 の機器 71 の送信部 (図では示していない) を介して、第 2 の機器 72 に送信する。第 2 の機器 72 ではこれを第 2 の暗号化 IC76 に渡す。

(2) ステップ (1) と同様に、第 2 の機器 72 の MPU75 において乱数 R2 (32 ビット) を生成して、記憶するとともに第 2 の機器 72 の送信部 (図では示していない) を介して、第 1 の機器 71 に送信する。第 1 の機器 71 ではこれを第 1 の暗号化 IC74 に渡す。

【0067】(3) 第 1 の暗号化 IC74 において、乱数 R3 (32 ビット) を生成して、外部よりアクセスできない領域に格納する。前記第 2 の機器 72 から受信した乱数 R2 と前記乱数 R3 とを結合して E 関数で暗号化する。暗号化には第 1 の暗号化 IC74 及び第 2 の暗号化 IC76 で予め共通に保持している秘密の認証鍵 S を用

いる。第 1 の暗号化 IC74 は、暗号化結果 C1 (64 ビット) を第 2 の機器 72 に送信する。

【0068】(4) ステップ (3) と同様に、第 2 の暗号化 IC76 において、乱数 R4 (32 ビット) を生成して、外部よりアクセスできない領域に格納する。前記第 1 の機器 71 から受信した乱数 R1 と前記乱数 R4 を結合して逆変換アルゴリズム D で復号化する。復号には前記認証鍵 S を用いる。第 2 の暗号化 IC76 は、復号結果 C2 (64 ビット) を第 1 の機器 71 に送信する。

【0069】(5) 第 1 の暗号化 IC74 において、前記第 2 の暗号化 IC76 から受信した復号文 C2 を前記 E 関数を用いて前記認証鍵 S で暗号化する。その結果の 64 ビットデータのうち上位 32 ビットを分離データ RR1、下位 32 ビットを分離データ RR4 とする。そして分離データ RR1 は第 1 の機器 71 の MPU73 に渡し、一方分離データ RR4 は外に出さずに第 1 の暗号化 IC74 内の外部からアクセスできない領域に格納する。

【0070】なお、第 1、第 2 の暗号化 IC76 が互いに正規なものであり同じ認証鍵 S を保持している場合には、前記分離データ RR1 は前記第 1 の機器 71 の MPU73 が生成した乱数 R1 と同じになり、前記分離データ RR4 は第 2 の暗号化 IC76 が生成した乱数 R4 と同じになる。

(6) ステップ (6) と同様に、第 2 の暗号化 IC76 において、前記第 1 の暗号化 IC74 から受信した暗号文 C1 を前記逆変換アルゴリズム D を用いて前記認証鍵 S で復号化する。その結果の 64 ビットデータの上位 32 ビットを分離データ RR2、下位 32 ビットを分離データ RR3 とする。そして分離データ RR2 は第 2 の機器 72 の MPU75 に渡し、一方分離データ RR3 は外に出さずに第 2 の暗号化 IC76 内の外部からアクセスできない領域に格納する。

【0071】なお、第 1、第 2 の暗号化 IC76 が互いに正規なものであり同じ認証鍵 S を保持している場合には、前記分離データ RR2 は前記第 2 の機器 72 の MPU75 が生成した乱数 R2 と同じになり、前記分離データ RR3 は第 1 の暗号化 IC74 が生成した乱数 R3 と同じになる。

(7) 第 1 の機器 71 の MPU73 において前記記憶していた R1 と前記第 1 の暗号化 IC74 から受け取った分離データ RR1 を比較して一致している場合には、第 2 の暗号化 IC76 及び第 2 の暗号化 IC76 が含まれた第 2 の機器 72 を正当な機器と認証する。

【0072】(8) ステップ (8) と同様に、第 2 の機器 72 の MPU75 において前記記憶していた R2 と前記第 2 の暗号化 IC76 から受け取った分離データ RR2 を比較して一致している場合には、第 1 の暗号化 IC74 及び第 1 の暗号化 IC74 が含まれた第 1 の機器 71 を正当な機器と認証する。

(9) 第1の暗号化IC74内で前記乱数R3と前記分離データRR4を用いてデータ転送鍵Kを作成する。図では双方の結合をデータ転送鍵K(64ビット)としている。

【0073】(10) ステップ(10)と同様に、第2の暗号化IC76内で前記分離データRR3と前記乱数R4を用いて第1の暗号化IC74と同様にデータ転送鍵Kを作成する。図では双方の結合をデータ転送鍵K(64ビット)としている。

(11) 第1の機器71の第1の暗号化IC74において、MPU73から送られてくるブロック化されたデジタル著作物mj(64ビット)を上記ステップ(9)で得られたデータ転送鍵Kを用いて暗号化し、得られた暗号文Cjを第2の機器72に送信する処理を、転送すべき全てのデジタル著作物を送信し終えるまで繰り返す。

【0074】(12) ステップ(11)に対応して、第2の機器72の第2の暗号化IC76において、第1の機器71が送信した暗号化された上記デジタル著作物Cj(64ビット)を受信し、上記ステップ(10)で得られたデータ転送鍵Kを用いて復号化し、得られたデジタル著作物mmjをMPU75に送る。この復号化は上記デジタル著作物Cjが第1の機器71から送信されてくる限り繰り返す。

【0075】このようにして、実施の形態2の暗号化装置により、実施の形態1の場合と同様に、第1の機器71と第2の機器72間で相互認証とデータ転送鍵Kの共有化とデータの暗号通信とが行われる。なお、上述したように、本実施の形態の暗号化装置と実施の形態1のものとはハードウェア構成において一致し、処理手順、即ち、各ハードウェア構成要素の接続と実行順序が異なるだけである。従って、本実施形態の暗号化装置の特徴やその変形例については、実施の形態1の場合と同様のことが言える。

(実施の形態3) 以上の実施の形態1及び2の暗号化装置には以下の共通点がある。

(1) 双方の機器においてそれぞれ2つの乱数が生成され、その一方は認証用のみ使用され、他の一方はデータ転送鍵Kの生成用のみ使用される。

(2) データ転送鍵Kの生成に使用される乱数はそのままの形で暗号化ICの外部に出力されることはなく、一方、認証用に使用される乱数は暗号化ICの外部に出力されて公開される。

【0076】これに対して、次に説明する実施の形態3の暗号化装置は、乱数を一つだけ生成し、それを認証用とデータ転送鍵の生成用の両方の目的に使用する。これは、実施の形態1及び2に比べて、暗号化IC内の乱数生成の負担を軽減するためである。また、暗号化ICの内部において認証のための乱数生成と比較処理を行う。即ち、実施の形態1及び2と相違し、データ転送鍵の生成のみならず認証処理も含めて暗号化ICの内部回

路で行う。これは、上述したように、暗号化ICを暗号解読のために用いるという悪用に対処するためであり、暗号通信の安全性を高めることができる。

【0077】図4は、本発明に係る暗号化装置を備えた第1の機器71と第2の機器72間で相互認証とデータ転送鍵の共有化とデータの暗号通信とを行う実施の形態3における処理シーケンスを示す図である。図4では、第1の機器81から第2の機器82にデジタル著作物mjを転送する場合が示されている。

【0078】なお、本実施の形態においても、実施の形態1及び2と同様に、各機器81、82に備えられた本発明に係る暗号化装置は、大きく分けてMPU83、85と暗号化IC84、86とから構成される。しかし、MPU83、85はデジタル著作物mjを暗号化IC84、86に渡すだけの機能を果たすので、実質的には、本発明に係る暗号化装置は暗号化IC84、86のみから構成されると言える。

【0079】第1の暗号化IC84及び第2の暗号化IC86は、実の形態1及び2と同様、1チップの半導体ICである。以下、図4に示されたステップ番号に従って、実施の形態3における暗号化装置の動作を説明する。

(1) 第1の暗号化IC84において乱数R1を生成して記憶するとともに、これをE関数で暗号化して第1の機器81の送信部(図では示していない)を介して、暗号文C1を第2の機器82に送信する。暗号化には第2の暗号化IC86と予め共通に保持している秘密の認証鍵Sを用いる。第2の機器82では受信した暗号文C1を第2の暗号化IC86に渡す。

【0080】(2) 第2の暗号化IC86では受信した暗号文C1を逆変換アルゴリズムDで復号化し復号文RR1を得る。第1の暗号化IC84及び第2の暗号化IC86が正規のものである場合にはこの復号文RR1は前記乱数R1と一致する。

(3) 第2の暗号化IC86において乱数R2を生成して記憶すると共に、これを前記復号文RR1と結合して前記逆変換アルゴリズムDで復号化する。復号には前記認証鍵Sを用いる。第2の暗号化IC86は復号文C2を第2の機器82の送信部(図では示していない)を介して、第1の機器81に送信する。第1の機器81ではこれを第1の暗号化IC84に渡す。

【0081】(4) 第1の暗号化IC84においては、前記復号文C2を前記E関数で暗号化し、その結果を分離データRRR1と分離データRR2に分離する。なお分離データRRR1は正当な機器でのやり取りの場合であれば、前記復号文RR1及び乱数R1と一致する。また分離データRR2は前記乱数R2と一致する。

(5) 第1の暗号化IC84内において、前記ステップ(1)で記憶していた乱数R1と前記分離データRRR1とを比較し、一致する場合には第2の暗号化IC86及

10

20

30

40

50

び第2の暗号化IC86を含んだ第2の機器82の正当性を認証する。

【0082】(6) 第1の暗号化IC84において、前記分離データRR2を前記E関数で暗号化し、第2の機器82に送信する。第2の機器82はこの暗号文C3を第2の暗号化IC86に渡す。

(7) 第2の暗号化IC86において、前記暗号文C3を前記逆変換アルゴリズムDで復号化し、復号文RRR2を得る。

【0083】(8) 第2の暗号化IC86において、前記ステップ(3)で記憶していた乱数R2と前記復号文RRR2を比較し、一致している場合には第1の暗号化IC84及び第1の暗号化IC84を含んだ第1の機器81の正当性を認証する。

(9) 第1の暗号化IC84において、前記乱数R1と前記分離データRR2を結合することでデータ転送鍵Kを生成する。

【0084】(10) 第2の暗号化IC86において、前記復号文RR1と前記乱数R2を用いてデータ転送鍵Kを生成する。

(11) 第1の機器81の第1の暗号化IC84において、MPU83から送られてくるブロック化されたデジタル著作物mj(64ビット)を上記ステップ(9)で得られたデータ転送鍵Kを用いて暗号化し、得られた暗号文Cjを第2の機器82に送信する処理を、転送すべき全てのデジタル著作物を送信し終えるまで繰り返す。

【0085】(12) ステップ(11)に対応して、第2の機器82の第2の暗号化IC86において、第1の機器81が送信した暗号化された上記デジタル著作物Cj(64ビット)を受信し、上記ステップ(10)で得られたデータ転送鍵Kを用いて復号化し、得られたデジタル著作物mmjをMPU85に送る。この復号化は上記デジタル著作物Cjが第1の機器81から送信されてくる限り繰り返す。

【0086】このようにして、実施の形態3の暗号化装置により、実施の形態1及び2の場合と同様に、第1の機器71と第2の機器72間で相互認証とデータ転送鍵Kの共有化とデータの暗号通信とが行われる。なお、上記ステップ(1)(2)(6)(7)においては1つの乱数の暗号化、ステップ(3)(4)においては2つの乱数の結合の暗号化を行っている。64ビット幅のE関数と逆変換アルゴリズムDを用いる場合には、各乱数を32ビットとして、前者については残りの32ビットの入力に固定の32ビットの値をパディングするとよい。例えば、乱数を下位32ビットとし、上位32ビットを固定的に全てゼロとする等である。また後者については結合した64ビットをそのまま各関数に入力するとよい。

【0087】また、各乱数のビット長を倍の64ビットにする場合には、前者はそのまま関数に入力し、後者については各関数を2回繰り返して用い、例えばCBCモ

ードのように連鎖のある暗号を行えばよい。以上述べた実施の形態3においては、実施の形態1及び2とは異なり、認証のための乱数とデータ転送鍵の共有化のための乱数は兼用されている。そして、認証のための乱数生成や認証のための比較処理は暗号化IC内で行われている。従って、乱数はそのままでは暗号化ICの外に現れないため、暗号化ICを解読器として用いる攻撃に対して、より安全である。また、このことにより、各乱数のビット数が少なくても十分な安全性を確保することができ

(実施の形態4) 次に、実施の形態4に係る暗号化装置について説明する。

【0088】本装置は、暗号化ICのコンパクト化を追求した実施形態であり、一方向認証を採用している点、及び、データ転送鍵が公開される点において、上記実施の形態1〜3と相違する。但し、暗号アルゴリズムE及びその逆変換アルゴリズムDは秘密にされていることを前提とする。図5は、第1の機器91から第2の機器92にデジタル著作物mjを転送する場合の処理シーケンスを示す図である。

【0089】図6は、第1の暗号化IC94のハードウェア構成を示すブロック図である。

(1) まず、第1の暗号化IC94の乱数生成部101はチャレンジデータとデータ転送鍵を兼用する乱数R1を生成し、乱数格納部102に格納すると共に、外部I/F部100を介して第2の機器92に送信する。

(2) 第2の暗号化IC96は、受信した乱数R1に対して、予め第1の暗号化IC94と共通に所有している認証鍵Sを用いて復号化し、得られた復号文C1を第1の機器91に送信する。

【0090】(3) 第1の暗号化IC94では、E関数106は、外部I/F部100及びスイッチ105を介して受信した復号文C1に対して、認証鍵S格納部103に予め格納された上記認証鍵Sと同じものを用いて暗号化する。その結果得られたデータRR1は、スイッチ107を経て比較部108に送られ、ここで、乱数格納部102に保持されていた乱数R1と比較される。

【0091】(4) その結果一致している場合には、第2の機器92は正当な機器であると認証できるので、比較部108は、乱数格納部102に保持されていた乱数R1がデータ転送鍵として用いられるように、スイッチ104を制御する。

(5) E関数106は、MPU93から外部I/F部100及びスイッチ105を経て送られてくるデジタル著作物mjに対して、スイッチ104を経て送られてくる乱数R1を用いて暗号化し、スイッチ107及び外部I/F部100を介して第2の機器92に送信する。

【0092】(6) 第2の機器92の第2の暗号化IC96においては、第1の機器91から送られてきたデジタル著作物Cjに対して、上記ステップ(2)で受信した乱

20

30

40

50

数R1をデータ転送鍵として用いて復号化し、得られたデジタル著作物mmjをMPU95に送る。このようにして、本実施の形態では、実施の形態1～3の場合よりも少ないステップと構成要素により、認証とデータ転送鍵の共有化と暗号通信とが実現される。

【0093】なお、本実施の形態では、第1の機器91から第2の機器92に送信された乱数R1がそのままデータ転送鍵として用いられているために、データ転送鍵は容易に第3者に知られ得る。ところが、そのデータ転送鍵を知った第3者がデジタル著作物Cjを盗聴し復号化しようとしても、上述したように暗号アルゴリズムE及びその逆変換アルゴリズムDは秘密にされているので、その試みは成功しない。

【0094】また、その第3者が都合のよい乱数R1を偽造することで暗号アルゴリズムを解読しようとしても、新たな乱数R1を乱数格納部102に格納できるのは乱数生成部101だけであり、この第1の暗号化IC94の外部から新たな乱数R1を乱数生成部101に格納する手段は存在しないので、その試みも成功しない。このように、暗号アルゴリズム及びその逆変換アルゴリズムが秘密にされるならば、本実施の形態のようなコンパクトな暗号化ICによっても認証とデータ転送鍵の生成と暗号通信を実現することができる。

【0095】なお、上記実施の形態1～4において、認証鍵Sを暗号化ICに設定する（記憶させる）方法としては以下が好ましい。つまり、認証鍵Sの一部は暗号化ICの製造時に予め設定しておき、残る部分はその暗号化ICの製造後に書き込む方法である。具体的には、認証鍵S格納部64の一部は、認証鍵Sの一部を予め書き込んだマスクROMで構成し、残る部分は、プログラマブルに書き込み可能な追記ROMで構成する。

【0096】これは、マスクROMのみで構成した場合には、最終的な暗号化ICの作成のために人手を介さないために安全である反面、リバースエンジニアリングによるチップ解析で設定値の解析が容易であるという欠点があり、一方、追記ROMのみで構成した場合には、設定値のリバースエンジニアリングによる解析が困難である反面、設定に人手を介するためミスが混入したり不正が可能となるという欠点があるので、それら両方の欠点を補うためである。

【0097】また、上記実施の形態1～4の暗号通信における暗号アルゴリズムの具体例として、次のようなものであってもよい。送信側でデジタル著作物を64ビットのブロックに分割し、前記データ転送鍵K（64ビット）とビットごとの排他的論理和をとる。その結果を暗号文とする。受信側でも同様に、受信した64ビットの暗号文とデータ転送鍵Kとの排他的論理和をとればよい。これによって、もとのブロックに復号される。

【0098】また、データ転送鍵Kを固定とするのではなく、それらブロックごとに、用いられるデータ転送鍵

Kを送信側と受信側で同期をとりながら更新していく方法もある。その更新のために、前記E関数や逆変換アルゴリズムDを用いてもよい。ブロック内の暗号／復号は先に述べた排他的論理和であってよい。また、上記実施の形態1～4において、認証方法としてチャレンジレスポンス型のいくつかの例が示されているが、本発明はこれらの例に限られない。例えば、認証側の暗号化ICで乱数を生成し、これをチャレンジデータとして送付し、証明側から返送されたレスポンスデータと認証側で生成した参照用のレスポンスデータとを比較する、というチャレンジレスポンス型の別の例であってよい。

【0099】なお、上記実施の形態1～4において、小さな回路規模で認証と暗号通信を安全に行なう技術を開示したが、安全性の強度とそのために必要な回路規模とはトレードオフの関係にあることは言うまでもない。従って、もしMPUや暗号化IC内に実装できる回路規模に余裕がある場合には、以下の目的のために、データ変換F（）を実行する新たな変換手段を追加導入することで、暗号通信の安全性を強化することができる。

(1) その一つは、平文のチャレンジデータや平文のレスポンスデータが伝送路を流れないようにすることである。

【0100】例えば、図1に示された第1の機器51が第2の機器52を認証する処理シーケンス（ステップ(1)(3)(6)(7)）において、以下のように変更する。ステップ(6)において、第2の暗号化IC56は、分離データRR1をMPU53に送るのではなく、その分離データRR1に所定の変換F（）を施し、その結果得られたデータF（RR1）をMPU53に送る。

【0101】ステップ(7)において、MPU53は、乱数R1と分離データRR1とを比較するのではなく、乱数R1に上記ステップ(6)で用いたものと同じ変換F（）を施し、その結果得られたデータF（R1）と第2の暗号化IC56から送られてきたデータF（RR1）とを比較する。このようにすることで、暗号文C1とその平文の一部RR1とが伝送路を流れることが回避されるので、既知平文攻撃に対する安全性が強化される。

(2) もう一つは、チャレンジデータをそのままデータ転送鍵として用いないようにすることである。

【0102】例えば、図5に示されたステップ(5)において、第1の暗号化IC94は、乱数R1をそのままデータ転送鍵として用いるのではなく、乱数R1に所定の変換F（）を施し、その結果得られたデータF（R1）をデータ転送鍵として用いる。同様に、ステップ(6)において、第2の暗号化IC96は、乱数R1をそのままデータ転送鍵として用いるのではなく、乱数R1に上記ステップ(5)で用いたものと同じ変換F（）を施し、その結果得られたデータF（R1）をデータ転送鍵として用いる。

10

20

30

40

50

【0103】このようにすることで、データ転送鍵F(R1)を秘匿することができ、暗号通信の安全性が強化される。

(3) さらにもう一つは、結合処理を複雑にすることである。例えば、図1に示されたステップ(9)において、第1の暗号化IC54は、乱数R3と分離データRR4とを単に桁方向に結合するのではなく、これらR3、RR4に所定の変換F()を施し、その結果得られたデータF(R3, RR4)をデータ転送鍵Kとする。

【0104】同様に、ステップ(10)において、第2の暗号化IC56は、乱数R4と分離データRR3とを単に桁方向に結合するのではなく、これらR4、RR3に上記ステップ(9)で用いたものと同じ変換F()を施し、その結果得られたデータF(R3, RR4)をデータ転送鍵Kとする。このようにすることで、データ転送鍵Kの生成手順が複雑化され、暗号通信の安全性が強化される。

(具体的な通信システムへの適応例) 以上のように、本発明に係る暗号化装置は、規模の小さな暗号化ICを備え、機器間通信の安全性を確保するための必要最小限の機能を持っている。従って、本暗号化装置は、秘密通信が必要とされ、かつ、小型であることが要求される通信機器、例えば、携帯電話機やデジタル著作物を扱うマルチメディア関連機器等に好適な装置である。

【0105】図7は、本発明に係る暗号化装置の具体的な通信システムへの適用例を示す図であり、映画等のデジタル著作物の再生システムの概観を示す。このシステムは、上記実施形態における第1の機器に対応する光ディスクドライブ装置110と第2の機器に対応する映像再生装置111とそれらを接続するSCSIケーブル116等からなる。光ディスクドライブ装置110で読み出した圧縮映像データを暗号化して映像再生装置111に転送し、そこで映像再生するシステムである。

【0106】図8は、光ディスクドライブ装置110の構成を示すブロック図である。光ディスクドライブ装置110は、装置全体の制御を行うMPU124と、映像再生装置111との通信インタフェースであるSCSIコントローラ121と、光ヘッド125を制御して光ディスク115から映像データを読み出し制御する読み出し制御部122と、上述の実施形態1~4における第1の機器の暗号化ICに相当する暗号化IC123とからなり、映像再生装置111が正当な機器であることを認証した後に、光ディスク115に記録された映像データを読み出して暗号化IC123において暗号化し、SCSIケーブル116を介して映像再生装置111に転送する。

【0107】図9は、光ディスクドライブ装置110の内部に実装される回路基板の概観を示す図である。暗号化IC123は、1個のシリコン基板に形成されたLSIであり、プラスチックでモールドされたフラットパッ

ケージの形状をしている。図10は、映像再生装置111の構成を示すブロック図である。映像再生装置111は、装置全体の制御を行うMPU131と、光ディスクドライブ装置110との通信インタフェースであるSCSIコントローラ130と、上述の実施形態1~4の第2の機器の暗号化ICに相当する暗号化IC132と、暗号化IC132で復号された圧縮映像データの伸長を行うMPEGデコーダ133と、伸長された映像データをアナログ映像信号に変換してCRT112及びスピーカ114に映像出力するAV信号処理部134とから構成される。

【0108】本発明に係る暗号化装置をこのような映像再生システムに適用することで、光ディスク115に記録されたデジタル著作物は不正コピー等から保護され、マルチメディア関連製品の流通市場における健全な発展が期待できる。

【0109】

【発明の効果】以上の説明から明らかなように、本発明に係る暗号化装置は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう機器に備えられる暗号化装置であって、前記データ転送鍵の共有化のための第1乱数を生成する第1乱数生成手段と、前記第1乱数生成手段により生成された第1乱数を保持する第1乱数保持手段と、前記第1乱数生成手段により生成された第1乱数を前記暗号通信の相手機器に送信する第1送信手段と、前記第1乱数保持手段に保持された第1乱数を用いて時変の前記データ転送鍵を生成するデータ転送鍵生成手段と、暗号通信の対象となる転送データに対して前記データ転送鍵を用いて暗号化する転送データ暗号化手段とを備え、前記第1乱数生成手段、前記第1乱数保持手段、前記データ転送鍵生成手段及び前記転送データ暗号化手段は、1個のIC内の回路で実現され、前記第1乱数保持手段は、前記ICの外部からアクセスできない領域に前記第1乱数を保持することを特徴とする。

【0110】これにより、データ転送鍵の生成に直接関連する第1乱数は外部からアクセスできない暗号化ICの内部に保持されるので、時変のデータ転送鍵は各機器に安全に共有され、暗号通信が行われる。また、暗号化ICは、機器間通信の安全性を確保するための必要最小限の機能を持つので、小さな回路で実現することができる。

【0111】ここで、前記暗号化装置はさらに、前記第1乱数生成手段により生成された第1乱数を暗号化する第1暗号化手段を備え、前記第1暗号化手段は、前記IC内の回路で実現され、前記第1送信手段は、前記第1暗号化手段で暗号化された第1乱数を前記相手機器に送信するとすることもできる。これにより、第3者はデータ転送鍵の生成に直接関連する第1乱数を知ることができなくなるので、データ転送鍵の秘密性が維持され、たとえ暗号アルゴリズム及びその逆変換アルゴリズムが知

られたとしても暗号通信は維持される。

【0112】ここで、前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記相手機器に送信するチャレンジデータ用の第2乱数を生成する第2乱数生成手段と、前記チャレンジデータに対して前記相手機器から返信されてきたレスポンスデータと前記第2乱数とが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証する認証手段とを備え、前記データ転送鍵生成手段は、前記認証がなされた場合に前記データ転送鍵を生成するとすることもできる。

【0113】これにより、機器間の相互認証が成功したときに同時に正規のデータ転送鍵が生成されることになり、秘密通信の安全性が向上される。ここで、前記第2乱数生成手段及び前記認証手段は、前記IC外の回路で実現されているとすることもできる。これにより、通信システムの安全性に関連しない部分、即ち、データ転送鍵の生成に直接関連しない処理部は暗号化ICの外に設けられるので、暗号化ICの規模が不要に大きくなるこ

とが抑制される。

【0114】ここで、前記暗号化装置はさらに、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段と、前記第1分離データを前記相手機器に返信する第2送信手段とを備え、前記第1暗号化手段は、前記第1乱数と前記第2乱数とを結合し、その結果得られた結合データを暗号化し、前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段及び前記分離手段は、前記IC内の回路で実現されているとすることもできる。

【0115】また、前記暗号化装置はさらに、前記第2乱数をチャレンジデータとして前記相手機器に送信する第2送信手段と、前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段とを備え、前記認証手段は、前記第1分離データを前記相手機器から返信されてきたレスポンスデータとして前記判断及び認証をし、前記第1暗号化手段は、前記相手機器から送信されてきたチャレンジデータと前記第1乱数とを結合し、その結果得られた結合データを暗号化し、前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段及び前記分離手段は、前記IC内の回路で実現されているとすることもできる。

【0116】これにより、機器間通信の安全性を確保するための必要最小限の機能を持ち、規模の小さな暗号化

ICを備えた暗号化装置が実現される。ここで、前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段及び前記復号化手段の少なくとも1つのものと同一であることを特徴とするとしてもできる。

【0117】これにより、転送データ暗号化手段と第1暗号化手段や復号化手段を1個の変換器で兼用して実装することが可能となるので、暗号化ICの回路規模が削減される。ここで、前記転送データ暗号化手段による暗号化のアルゴリズムは、前記第1暗号化手段及び前記復号化手段のいずれのものとも異なり、かつ、いずれのものよりも簡易であるとしてもできる。

【0118】これにより、転送データのサイズが大きいため何回もその暗号化を繰り返すような場合であっても、暗号化のためにデータ転送時間が大幅に長くなってしまいうという不具合が回避される。ここで、前記転送データ暗号化手段は、前記転送データを一定長のブロックに区切り、各ブロックに対して前記データ転送鍵の対応する部分を用いて暗号化するとすることもできる。

【0119】これにより、データサイズの大きい転送データの暗号通信に対しても、本暗号化装置を適用することが可能となる。ここで、前記転送データ暗号化手段は、前記ブロックと前記データ転送鍵の対応する部分との排他的論理和をとることにより、前記暗号化を行なうとすることもできる。

【0120】これにより、簡易な論理回路で転送データ暗号化手段を実現することが可能となる。ここで、前記第1暗号化手段での暗号と前記復号化手段での復号化とは、同一の変換アルゴリズムであるとしてもできる。これにより、第1暗号化手段と復号化手段を1個の変換器で兼用して実装することが可能となり、暗号化ICの回路規模が削減される。

【0121】ここで、前記第1暗号化手段及び前記復号化手段は、予め前記IC内に保持された鍵データを用いて前記暗号化及び復号化を行い、その鍵データの一部は、前記IC内のマスクROM領域に格納され、残る一部は、前記IC内の追記ROM領域に格納されているとすることもできる。これにより、認証鍵をマスクROMのみで構成した場合における欠点と、追記ROMのみで構成した場合における欠点と補うことが可能となる。

【0122】ここで、前記機器は、チャレンジレスポンス型の認証プロトコルに基づく通信により相互に前記相手機器が正当な機器であることを認証し合うものであり、前記暗号化装置はさらに、前記チャレンジデータに対して前記相手機器から送られてきた暗号化された結合データを復号化する復号化手段と、復号化された結合データをレスポンスデータに相当する第1分離データと残る第2分離データとに分離する分離手段と、前記第1乱数と前記第1分離データとが一致するか否かを判断し、一致した場合に前記相手機器は正当な機器であると認証

する認証手段と、前記認証がなされた場合に前記第2分離データを暗号化する第2暗号化手段と、暗号化された前記第2分離データをレスポンスデータとして前記相手機器に返信する第2送信手段とを備え、前記データ転送鍵生成手段は、前記第1乱数と前記第2分離データとを結合することにより、前記データ転送鍵を生成し、前記復号化手段、前記分離手段及び前記第2暗号化手段は、前記IC内の回路で実現されているとすることもできる。

【0123】これにより、乱数を一つだけ生成し、それを認証用とデータ転送鍵の生成用の両方の目的に使用しているため、暗号化装置での乱数生成のための回路規模が軽減される。また、暗号化ICの内部において認証のための乱数生成と比較処理を行っているため、暗号通信の安全性が高められる。

【0124】また、本発明は、データ転送鍵の共有化とそのデータ転送鍵を用いた暗号通信を行なう送信機及び受信機から構成される通信システムであって、それら送信機及び受信機が、それぞれ上記構成を備えることとすることもできる。これにより、送信機及び受信機間で相互認証が行われると共にデータ転送鍵が生成されること、データ転送鍵の生成に直接関連する乱数はそのままでは送受信されないこと、及び、データ転送鍵の生成に直接関連する2つの乱数はそれぞれ送信機及び受信機から提供されたものであることから、規模の小さな暗号化ICを用いて実現するのに好適であり、かつ、安全性の高い暗号通信システムが実現される。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図2】図1に示された第1の暗号化IC54のハードウェア構成を示すブロック図である。

【図3】本発明の第2の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図4】本発明の第3の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図5】本発明の第4の実施の形態に係る暗号化装置の処理シーケンスを示す図である。

【図6】図5に示された第1の暗号化IC94のハードウェア構成を示すブロック図である。

【図7】本発明に係る暗号化装置の具体的な通信システムへの適用例を示す図である。

【図8】図7に示された光ディスクドライブ装置110の構成を示すブロック図である。

【図9】同光ディスクドライブ装置110の内部に実装される回路基板の概観を示す図である。

【図10】図7に示された映像再生装置111の構成を示すブロック図である。

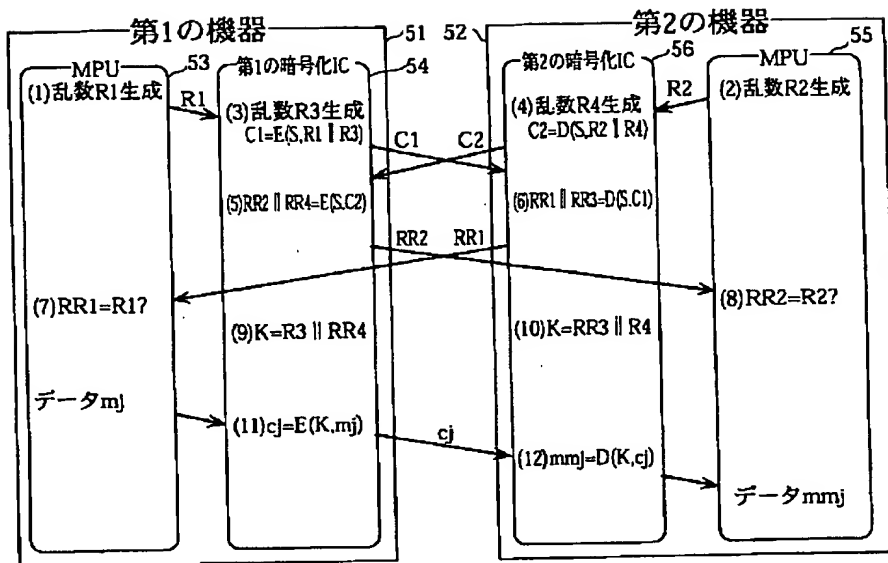
【図11】第1の従来技術に係る一方方向認証の処理シーケンスを示す図である。

【図12】第2の従来技術に係る双方方向認証の処理シーケンスを示す図である。

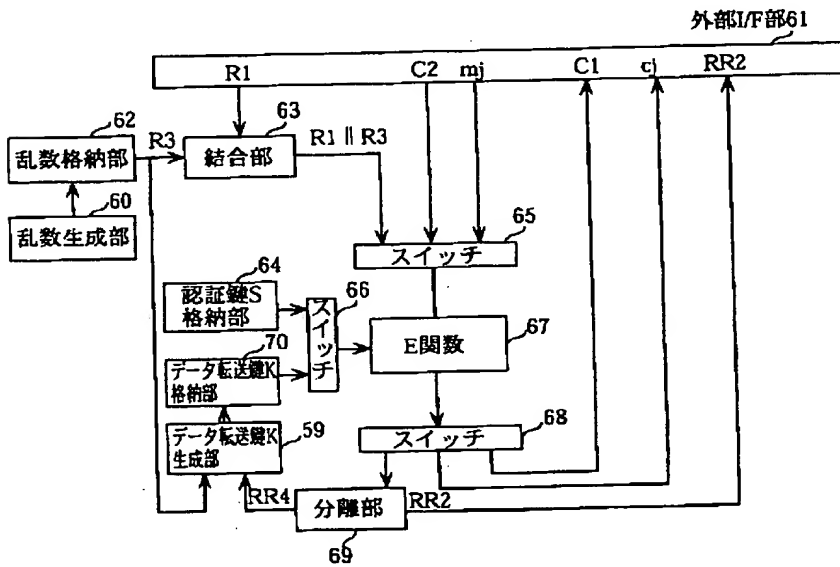
【符号の説明】

51、71、81、91	第1の機器
52、72、82、92	第2の機器
53、73、83、93	第1の機器のMPU
54、74、84、94	第1の暗号化IC
55、75、85、95	第2の機器のMPU
56、76、86、96	第2の暗号化IC
59	データ転送鍵K生成部
60、101	乱数生成部
61、100	外部I/F部
62、102	乱数格納部
63	結合部
64、103	認証鍵S格納部
65、66、68、104、105、107	スイッチ
67、106	E関数
69	分離部
70	データ転送鍵K格納部
108	比較部
110	光ディスクドライブ装置
111	映像再生装置
121	SCSIコントローラ
122	制御部
123	暗号化IC
124	MPU
125	光ヘッド
130	SCSIコントローラ
131	MPU
132	暗号化IC
133	MPEGデコーダ
134	AV信号処理部

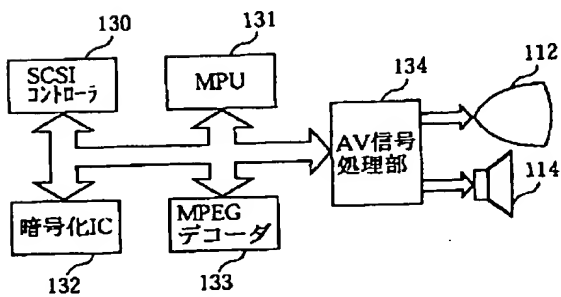
【図1】



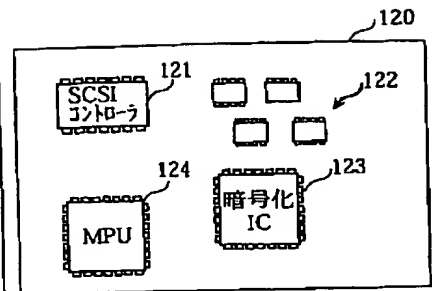
【図2】



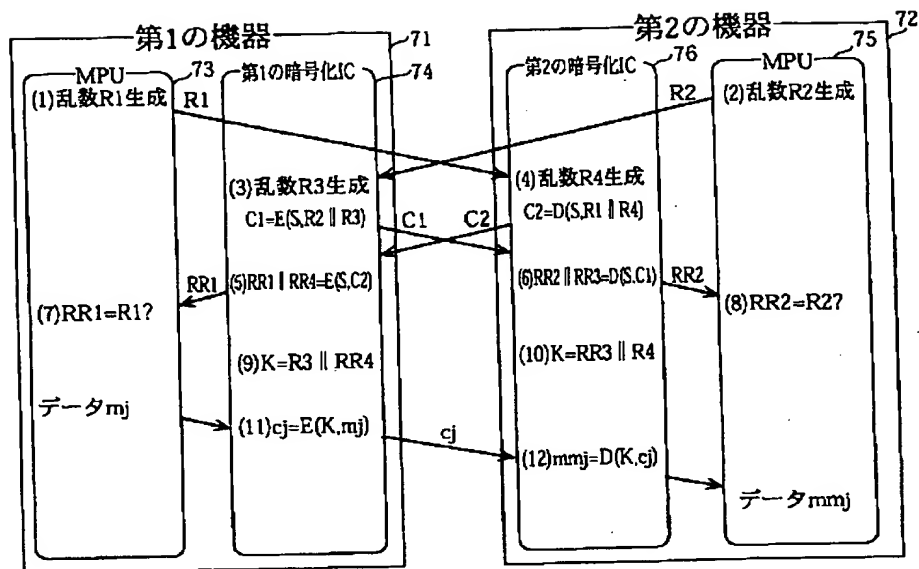
【図10】



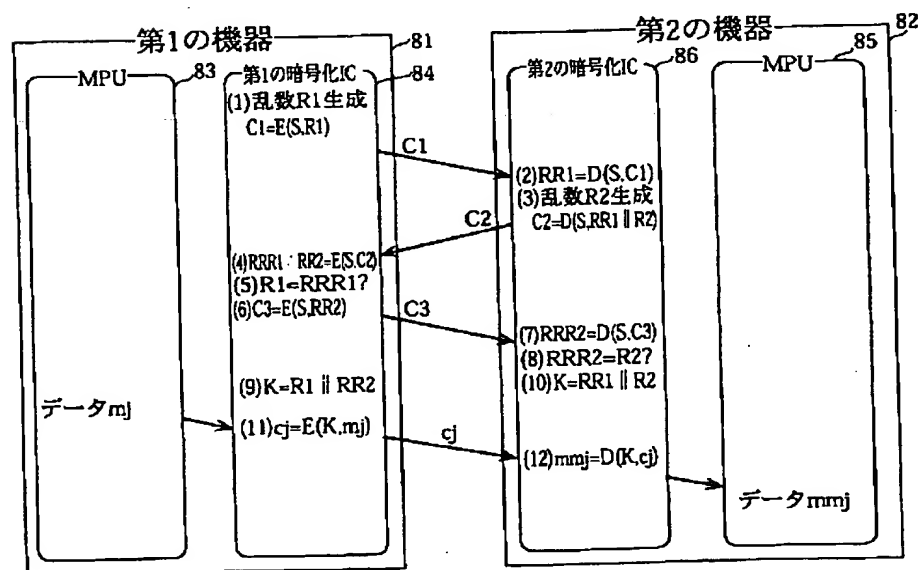
【図9】



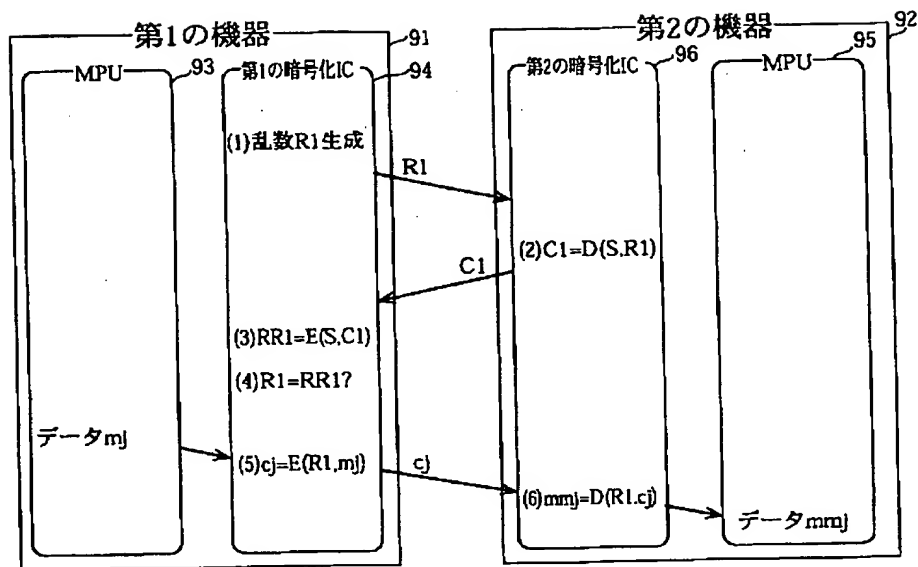
【図3】



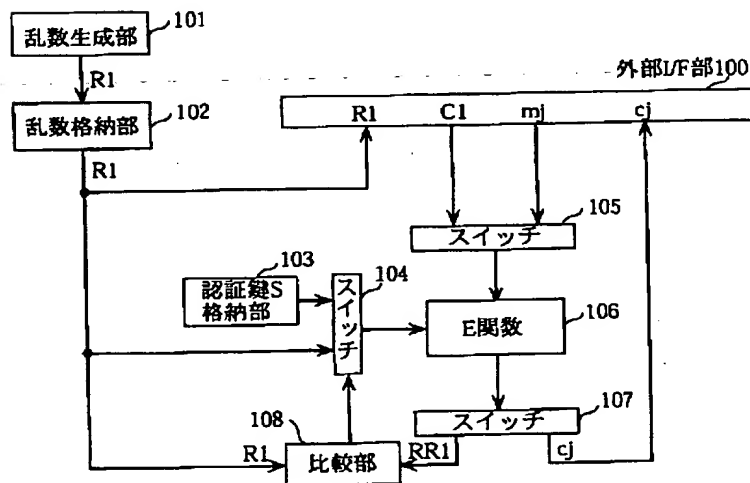
【図4】



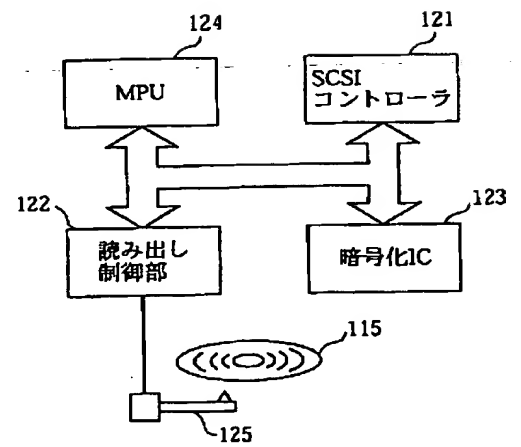
【図5】



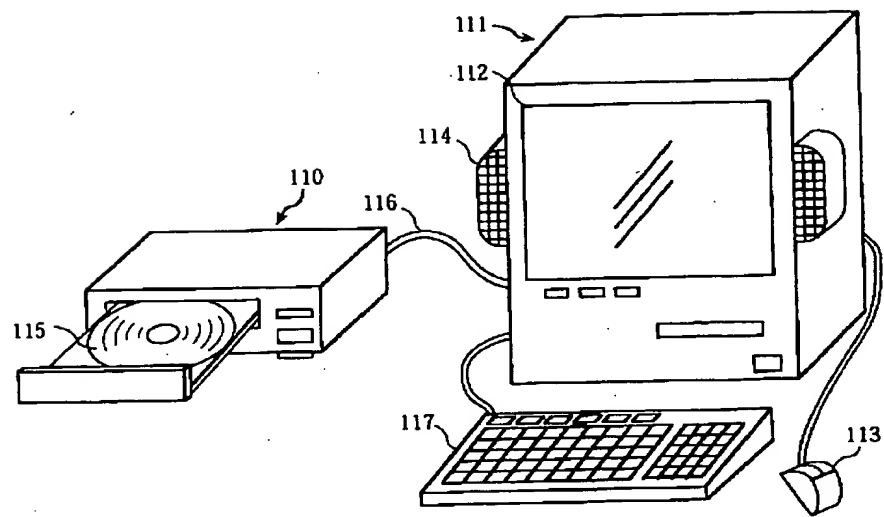
【図6】



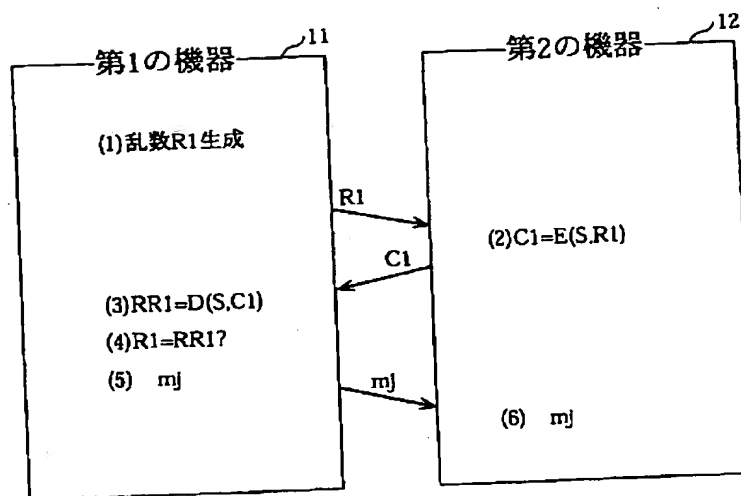
【図8】



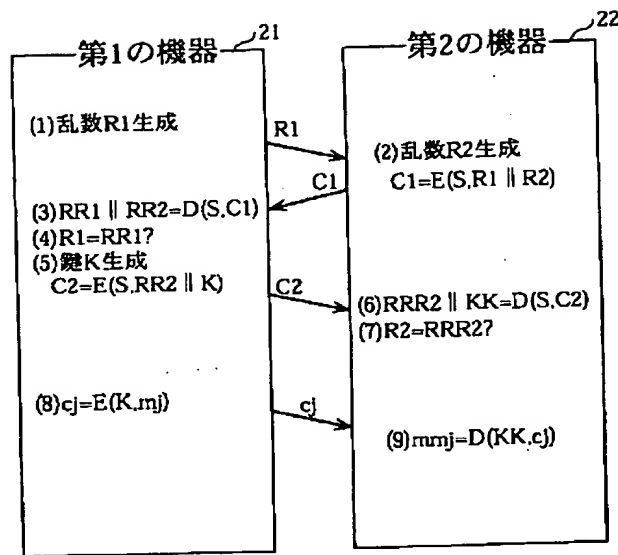
【図7】



【図11】



【図12】



フロントページの続き

(51) Int. Cl.⁶

識別記号

庁内整理番号

F I

H O 4 L 9/00

技術表示箇所

6 7 5 A